SÍLABO DE SEGURIDAD DE REDES

I. INFORMACIÓN GENERAL

PROGRAMA DE ESTUDIOS	ADMINISTRACIÓN DE CENTROS DE CÓMPUTO				
MÓDULO	OPERACIÓN DE LOS SERVICIOS DE TI				
DOCENTE		PERIODO ACADÉMICO	SEMESTRE	HORAS SEMANA	HORAS SEMESTRE
ERICK JINM BEJARANO TELLO		2024 - II	II	07	112

UNIDAD DIDÁCTICA	**MODALIDAD PRESENCIAL**					
	CRÉDITOS			**HORAS**		
	TEORÍA	**PRÁCTICA**	**TOTAL**	**TEORÍA**	**PRÁCTICA**	**TOTAL**
SEGURIDAD DE REDES	2	1	3	48	64	112

PROPÓSITO DE LA UNIDAD (Qué, cómo y para qué)	El propósito de la unidad didáctica tiene como objetivo proporcionar a los estudiantes un conocimiento fundamental sobre la seguridad de redes, abarcando conceptos clave, herramientas, técnicas, y mejores prácticas para proteger redes informáticas contra amenazas internas y externas. El aprendizaje se desarrollará mediante una combinación de clases teóricas, laboratorios prácticos, y actividades colaborativas. Los estudiantes participarán en talleres, simulaciones, y proyectos que les permitirán aplicar los conceptos teóricos a situaciones reales. Además, se utilizarán estudios de caso para analizar brechas de seguridad y discutir estrategias de mitigación. Las evaluaciones incluirán exámenes, ejercicios prácticos, y la elaboración de un proyecto integrador al final del curso. El propósito final de esta unidad didáctica es preparar a los estudiantes para enfrentar y gestionar los desafíos de la seguridad en redes, proporcionando las habilidades necesarias para proteger la infraestructura de red en entornos empresariales o personales. Al completar la unidad, los estudiantes estarán capacitados para implementar medidas preventivas, detectar y responder a incidentes de seguridad, y asegurar la continuidad de operaciones ante posibles amenazas cibernéticas.
UNIDAD DE COMPETENCIA	Realizar la puesta en producción de los sistemas de información o servicios de TI, de acuerdo a la planificación efectuada.

CAPACIDAD TERMINAL	**INDICADORES DE LOGRO**
• Implementar Seguridad de Redes en la Operación de Sistemas de Tecnología de Información según normas y políticas de la organización	Instala squid proxy server los sistemas de tecnología de información según las normas y políticas de la organización
	Implementa PKI Criptografía de Clave Pública en los Sistemas de Tecnología de Información según las normas y políticas de la organización
	Implementa Servicio HTTPS en los Sistemas de Tecnología de Información. según las normas y políticas de la organización

II. ORGANIZACIÓN DE ACTIVIDADES Y CONTENIDOS BASICOS

SEMANA	ELEMENTO DE CAPACIDAD	ACTIVIDADES DE APRENDIZAJE	CONTENIDOS			MEDIOS Y MATERIALES	HORAS	
			CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		TEORIA	PRACTICA
01 19/08/24	Capacidad para identificar y evaluar las amenazas y vulnerabilidades presentes en una red, analizando los posibles riesgos asociados y proponiendo medidas preventivas y correctivas.	Nº 01 Introducción a la Seguridad de Redes	Definición y objetivo de la seguridad de redes. Principales amenazas y vulnerabilidades en redes. Conceptos básicos: Confidencialidad, integridad, disponibilidad. Introducción a los tipos de ataques: Phishing, malware, DoS, etc.	Identificación y clasificación de amenazas en un entorno de red simulado. Discusión en clase sobre ejemplos recientes de brechas de seguridad. Taller para identificar amenazas en escenarios de redes simples.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
02 26/08/24		Nº 02 Fundamentos de Redes	Estructura de una red: LAN, WAN, VPN. Componentes básicos de redes: Routers, switches, firewalls. Modelos OSI y TCP/IP y su relación con la seguridad de redes.	Configuración básica de una red local (LAN). Verificación de la estructura de red utilizando herramientas básicas de diagnóstico. Práctica en laboratorio: Configuración de una red LAN simple. Análisis de tráfico de red usando Wireshark.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
03 02/09/24		Nº 03 Políticas de Seguridad de Redes	Importancia de las políticas de seguridad en redes. Elementos de una política de seguridad: Control de acceso, uso aceptable, gestión de parches. Normativas y estándares de seguridad: ISO/IEC 27001, NIST.	Desarrollo de una política de seguridad básica para una pequeña empresa. Creación de una política de seguridad de red para un escenario específico. Discusión sobre la implementación de políticas en diferentes tipos de redes.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
04 09/09/24		Nº 04 Control de Acceso y Autenticación	Métodos de autenticación: Contraseñas, autenticación multifactor (MFA), biometría.	Configuración de autenticación básica y control de acceso en un entorno de red.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo.	Google Classroom Microsoft Power Point Mentimenter Prezzi	03	04

SEMANA	ELEMENTO DE CAPACIDAD	ACTIVIDADES DE APRENDIZAJE	CONTENIDOS			MEDIOS Y MATERIALES	HORAS	
			CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		TEORIA	PRACTICA
				Taller: Configuración de contraseñas seguras y políticas de acceso. Simulación de ataques de fuerza bruta para entender la importancia de contraseñas seguras.	Responsabilidad en la ejecución.	Wireshark Cisco Packet Tracer Virtual Box		
05 16/09/24		Nº 05 Criptografía Básica	Introducción a la criptografía: Simétrica vs Asimétrica. Conceptos clave: Cifrado, descifrado, hashing. Algoritmos criptográficos comunes: AES, RSA, SHA-256.	Uso de herramientas de cifrado para proteger la información en tránsito. Ejercicios en clase para cifrar y descifrar mensajes utilizando herramientas básicas. Discusión sobre casos de uso de la criptografía en la vida real.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
06 23/09/24	Habilidad para configurar y administrar herramientas y tecnologías de seguridad, como firewalls, sistemas de detección de intrusiones (IDS/IPS), y protocolos de autenticación, con el fin de proteger la infraestructura de red.	Nº 06 Firewalls y Control de Tráfico de Red	Tipos de firewalls: Packet filtering, Stateful, Proxy, Next-Generation Firewalls (NGFW). Configuración básica de un firewall. Control de tráfico de red y filtrado de paquetes.	Configuración y prueba de reglas básicas de firewall en un entorno controlado. **Laboratorio:** Configuración de un firewall para bloquear tráfico no deseado. Simulación de un ataque y análisis de cómo un firewall puede mitigar el daño.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
07 30/09/24		Nº 07 Redes Privadas Virtuales (VPNs)	Conceptos básicos de VPNs y su rol en la seguridad de redes. Tipos de VPNs: Site-to-Site, Remote Access. Protocolos VPN: PPTP, L2TP, IPSec, SSL/TLS.	Configuración de una VPN básica para acceso remoto seguro. **Laboratorio:** Configuración de una VPN y prueba de conexión segura. Discusión sobre las ventajas y limitaciones de las VPNs.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
08 07/10/24		Nº 08	Riesgos de seguridad específicos en redes inalámbricas.	Configuración de una red inalámbrica segura utilizando WPA3.	Practica la puntualidad. Trabaja en equipo	Google Classroom Microsoft Power Point	03	04

SEMANA	ELEMENTO DE CAPACIDAD	ACTIVIDADES DE APRENDIZAJE	CONTENIDOS			MEDIOS Y MATERIALES	HORAS	
			CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		TEORIA	PRACTICA
		Seguridad en Redes Inalámbricas	Protocolos de seguridad Wi-Fi: WEP, WPA, WPA2, WPA3. Configuración segura de una red inalámbrica.	**Taller:** Configuración de un router inalámbrico con medidas de seguridad. Simulación de un ataque de red inalámbrica para demostrar vulnerabilidades comunes.	Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box		
09 14/10/24		Nº 09 Detección y Prevención de Intrusiones (IDS/IPS)	Diferencias entre IDS (Sistema de Detección de Intrusiones) y IPS (Sistema de Prevención de Intrusiones). Métodos de detección: Basados en firmas, análisis de comportamiento. Implementación de IDS/IPS en redes.	Configuración básica de un IDS/IPS en un entorno de red simulado. **Laboratorio:** Configuración y prueba de un sistema IDS en una red pequeña. Análisis de logs de IDS para identificar posibles intrusiones.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
10 21/10/24	Competencia para monitorear el tráfico de red y detectar actividades sospechosas, así como para responder de manera efectiva a incidentes de seguridad, mitigando daños y restaurando la operación normal de la red.	Nº 10 Seguridad en Aplicaciones y Servicios de Red	Vulnerabilidades en aplicaciones de red comunes: HTTP, FTP, DNS. Principios de seguridad en el desarrollo de aplicaciones. Configuración segura de servidores de aplicaciones.	Configuración de un servidor web con medidas de seguridad básicas. **Laboratorio:** Configuración de un servidor web seguro. Simulación de ataques a aplicaciones web y análisis de medidas de mitigación.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
11 28/10/24		Nº 11 Protección contra Malware y Ataques DDoS	Tipos de malware: Virus, gusanos, troyanos, ransomware. Métodos de propagación y prevención de malware. Detección y mitigación de ataques de denegación de servicio (DDoS).	Implementación de medidas de seguridad anti-malware y configuración de protección contra DDoS. Simulación de una infección por malware y su contención. Discusión sobre estrategias de mitigación de DDoS en redes.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
12 04/11/24		Nº 12	Importancia de la auditoría y el monitoreo continuo en la seguridad de redes.	Configuración de una herramienta básica de monitoreo de red.	Practica la puntualidad. Trabaja en equipo	Google Classroom Microsoft Power Point	03	04

SEMANA	ELEMENTO DE CAPACIDAD	ACTIVIDADES DE APRENDIZAJE	CONTENIDOS			MEDIOS Y MATERIALES	HORAS	
			CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		TEORIA	PRACTICA
		Auditoría y Monitoreo de Redes	Herramientas de monitoreo: SNMP, Syslog, Wireshark. Análisis de logs y respuesta a incidentes.	Laboratorio: Configuración de un sistema de monitoreo y análisis de logs. Ejercicio práctico: Respuesta a un incidente de seguridad detectado por el sistema de monitoreo.	Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box		
13 11/11/24	Capacidad para desarrollar y aplicar políticas y procedimientos de seguridad de redes, asegurando que todas las prácticas de seguridad estén alineadas con las normativas vigentes y las mejores prácticas de la industria.	Nº 13 Seguridad en la Nube y Servicios Remotos	Riesgos de seguridad específicos en entornos de nube. Medidas de seguridad en servicios cloud: IAM, cifrado, monitoreo. Consideraciones para la gestión segura de servicios remotos.	Configuración de medidas básicas de seguridad en un servicio cloud. Discusión sobre casos de brechas de seguridad en la nube. **Taller:** Implementación de políticas de seguridad en un servicio de nube pública.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
14 18/11/24		Nº 14 Seguridad Física y en la Capa de Red	Importancia de la seguridad física en la protección de redes. Medidas de seguridad en la capa de red: MAC filtering, IPsec. Configuración de seguridad en dispositivos de red: Routers, switches.	Implementación de medidas de seguridad física en una infraestructura de red simulada. **Taller:** Configuración de filtrado MAC y medidas de seguridad en un router. Discusión sobre la importancia de la seguridad física y sus desafíos.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
15 25/11/24		Nº 15 Gestión de Incidentes y Continuidad del Negocio	Proceso de gestión de incidentes de seguridad. Estrategias de recuperación y continuidad del negocio. Documentación y comunicación en respuesta a incidentes.	Desarrollo de un plan de respuesta a incidentes para un escenario específico. **Ejercicio práctico:** Simulación de un incidente de seguridad y desarrollo de un plan de respuesta. Presentación de un plan de continuidad del negocio en grupos.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04

SEMANA	ELEMENTO DE CAPACIDAD	ACTIVIDADES DE APRENDIZAJE	CONTENIDOS			MEDIOS Y MATERIALES	HORAS	
			CONCEPTUAL	PROCEDIMENTAL	ACTITUDINAL		TEORIA	PRACTICA
16 02/12/24		Nº 16 Revisión Final y Proyecto Integrador	Revisión de todos los temas vistos durante el curso. Integración de conceptos en un proyecto final.	Presentación y evaluación de proyectos finales. Examen final teórico y práctico. Presentación de proyectos: Implementación de un entorno de red seguro basado en los conocimientos adquiridos durante el curso.	Practica la puntualidad. Trabaja en equipo Demuestra cuidado limpieza de los equipos y el ambiente de cómputo. Responsabilidad en la ejecución.	Google Classroom Microsoft Power Point Mentimenter Prezzi Wireshark Cisco Packet Tracer Virtual Box	03	04
17 24/07/23	Retroalimentación							
18 31/07/23	Recuperación							

III. METODOLOGIA

PRESENCIAL

- Expositiva
- Plenaria
- Trabajo de grupo
- Demostrativa

NO PRESENCIAL

- Asincrónica: Classroom, WhatsApp, Correo Electrónico, (Para trabajos encargados, cuestionarios, foros, evaluaciones, materiales u otra)

IV. EVALUACION

- ✓ Evaluación de cumplimiento de reportes en la plataforma virtual
- ✓ Evaluaciones cognoscitivas
- ✓ Evaluación actitudinal
- ✓ Evaluaciones Prácticas
- ✓ informes de trabajos encargados

.

V. CONDICIONES DE APROBACION

- El calificativo mínimo aprobatorio es 13.
- En todos los casos la fracción 0.5, se considera como una unidad a favor del estudiante.
- Si el estudiante obtuviera nota menor a 10, en todos los casos, repite la unidad didáctica.
- El estudiante que acumulará inasistencias injustificadas en número igual o mayo al 30%, del total de horas programadas en la UD, será desaprobado automáticamente.

VI. REFERENCIAS BIBLIOGRAFICAS

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
- Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
- Andress, J. (2019). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice (3rd ed.). Syngress.
- Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5th ed.). Prentice Hall.
- Cole, E., & Krutz, R. L. (2020). Network Security Bible (2nd ed.). Wiley.

La Banda de Shilcayo, 19 de Agosto del 2024

V°B° Coordinador Programa de Estudios

Docente a cargo de la Unidad Didáctica